AppGate SDP and LDAP over SSL (LDAPS) Integration Guide

V2.1
Tested for use on versions:
AppGate SDP v4.3 or newer
Last updated: March 2020

TABLE OF CONTENTS

INTRODUCTION

AppGate SDP supports standard enterprise identity providers (IdP) such as Active Directory. These can be used to authenticate users connecting through the Client, and also to authenticate administrators signing in to the Controller admin UI.

BEFORE YOU START

Test topology

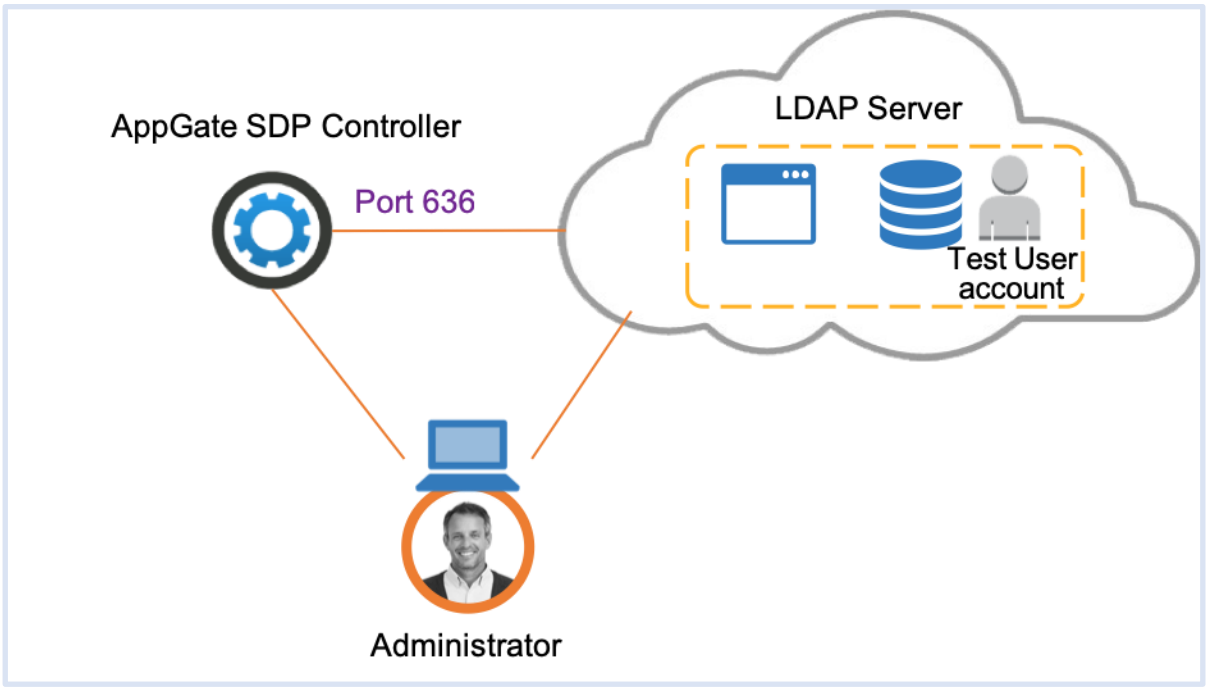


Figure 1: LDAPS integration test topology

This integration requires the following:

- A Microsoft Active Directory (AD) server, accessible on your browser and configured for LDAP over SSL. LDAP connections are not enabled by default. For details refer to Microsoft support
- Internet Information Services (IIS) and Certificate Services installed and running on your AD server
- An AppGate SDP Controller installed and accessible on your network. Information for setting up your Controller can be found in the Admin UI: https://sdphelp.cyxtera.com/adminguide/the-first-controller.html
- A test user account setup in your AD server database. The user account should include sAMAccountName, GivenName, sn and email address.

STEP BY STEP GUIDE TO INTEGRATION

1. AD SERVER CONFIGURATION: EXPORT THE CA CERTIFICATE

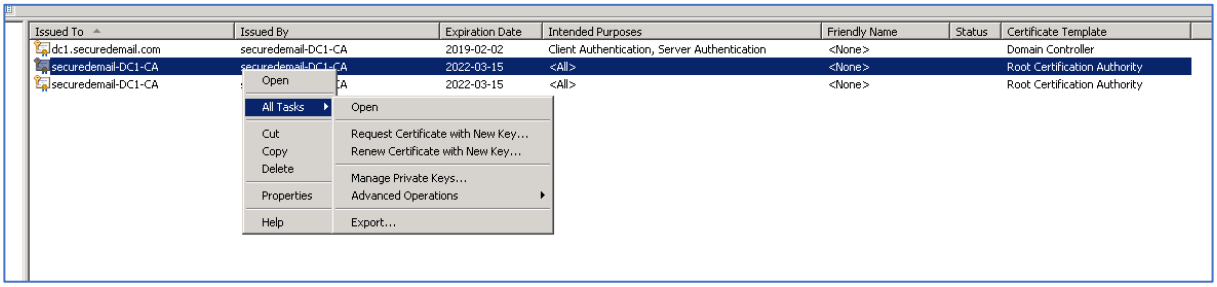
Install a CA certificate on your AD server

- On your AD server, use the IIS (Internet Information Services) tools to
  - Create a certificate request
  - Issue the CA certificate to your AD server
  - Install the CA certificate to your AD server certificate store

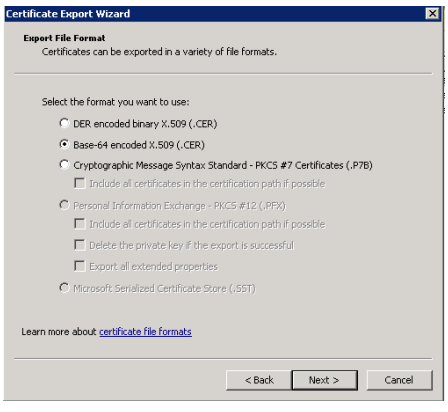
An example of how to do this is provided here: [Installing an SSL Certificate in Windows Server 2008 (IIS 7.0)]

Export the root CA certificate as Base-64 encoded format

- Select the root CA certificate from the certificate store
- Click <Export> to launch the Export Wizard



- On the Certificate Export Wizard window, select <**Base-64 encoded X.509**> format and follow the instructions



2. APPGATE SDP CONFIGURATION: ADD A NEW IDENTITY PROVIDER

In your AppGate SDP console, select System > Identity Providers

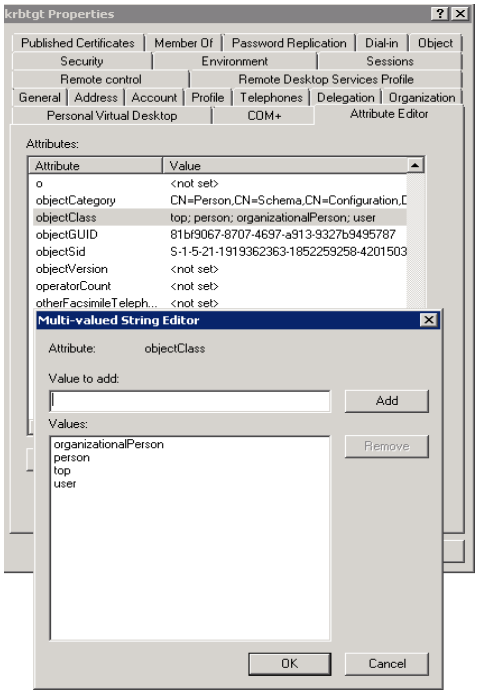
- create a new Identity Provider
- choose the type LDAP
- start configuring your identity provider. For the following fields enter the following information:
  - *IPv4Pool* –select default pool v4 from the drop down list
  - *Where to use* – tick both boxes for Client and Admin UI
  - *Hostnames or IP addresses* – IP address of your LDAP server host
  - *Port* - enter 636 for SSL
  - Enable SSL – tick this box

Upload the CA certificate:

- In System > Trusted Certificates choose +Add New. Below the Certificate field click the <Choose a File> button and upload the Certificate that you exported

The Certificate field should look something like this:

- To fill in the remaining fields on the Identity Provider Configuration form open your AD server Properties window to find the information required.



Note: the “Attribute Editor” tab may not be visible – steps to do this can be found here: https://activedirectoryfaq.com/2014/10/ad-attribute-editor-missing-make-search-visible/

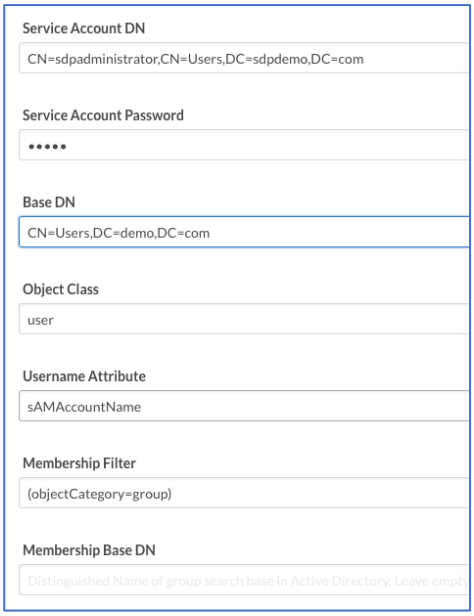
- Complete the following fields in the configuration form:
    - Service Account DN & Password – enter the credentials for the Controller to log into the AD database
      eg. CN=AppGate Service Account,OU=service,DC=company,DC=com
    - Base DN – enter the user search base on your AD server, typically 'Users';
      eg: CN=Users,DC=myldapserver,DC=com
    - Object Class = user
    - Username Attribute – leave as the default (sAMAccountName)
    - Membership Filter – leave as the default (objectCategory=group)
    - Membership Base DN – leave blank

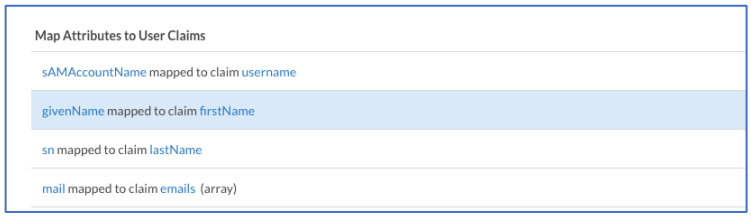
3. APPGATE SDP CONFIGURATION: MAPPING ATTRIBUTES

In your AppGate SDP console, finish configuring the identity provider form by mapping attributes.
In the <Map Attributes to User Claims> field:

- click <+ ADD NEW> to add each attribute mapping
- Complete each new attribute field to map the attributes in your AD database to the corresponding AppGate SDP claim names. For example:
    - attribute: "sAMAccountName" mapped to claim "username"
    - attribute: "givenName" mapped to claim "firstName"
    - *attribute:* "sn" mapped to *claim name "*lastName"

The completed fields in the form should look something like this:





4. TESTING INTEGRATION

There are two stages to testing integration.

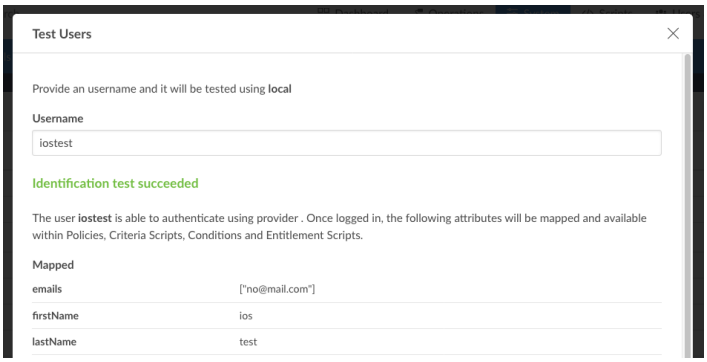
Test the connection with your LDAP server.

- After completing the Identity Provider form on the AppGate SDP console, click <SAVE>
- Click <TEST> to check the connections. You should see the following message confirming that the test has been successful:

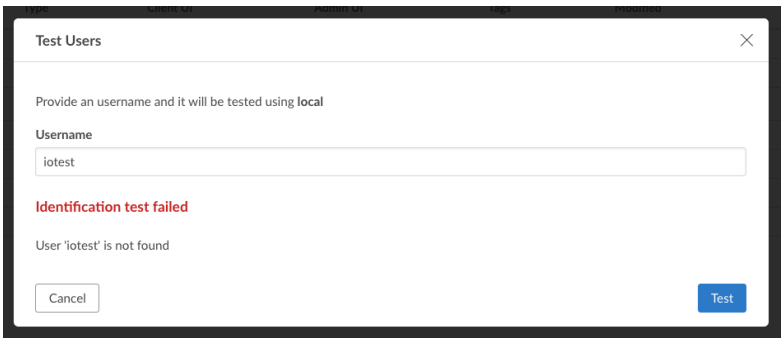
Test user authentication

- Return to the System>Identity Providers console
- Hover over the listing for your new LDAP identity provider:
  - click on the <Test User> icon on the right-hand side:
- In the pop-up window enter the username of the test user in your AD database

If AppGate SDP can successfully bind to the directory, the test will provide a list showing how the attributes map to the user-claims and the claim values that will be returned to the Controller.



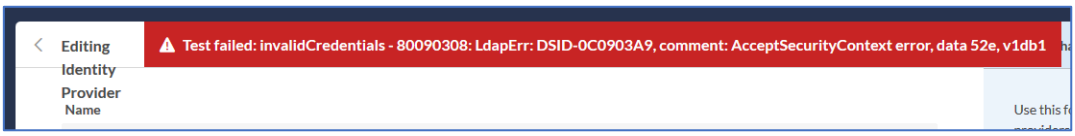
The following message is also an indicator that system integration has been successful: in this instance, AppGate SDP has been able to bind to the directory but there has been an error finding the username in AD". It might be because of a typing error or the user doesn't exist in configured BaseDN



TROUBLESHOOTING

Networking / connectivity error

- If there is a problem connecting to your Identity Provider you should see a <test failed> message on your AppGate SDP console, for example:

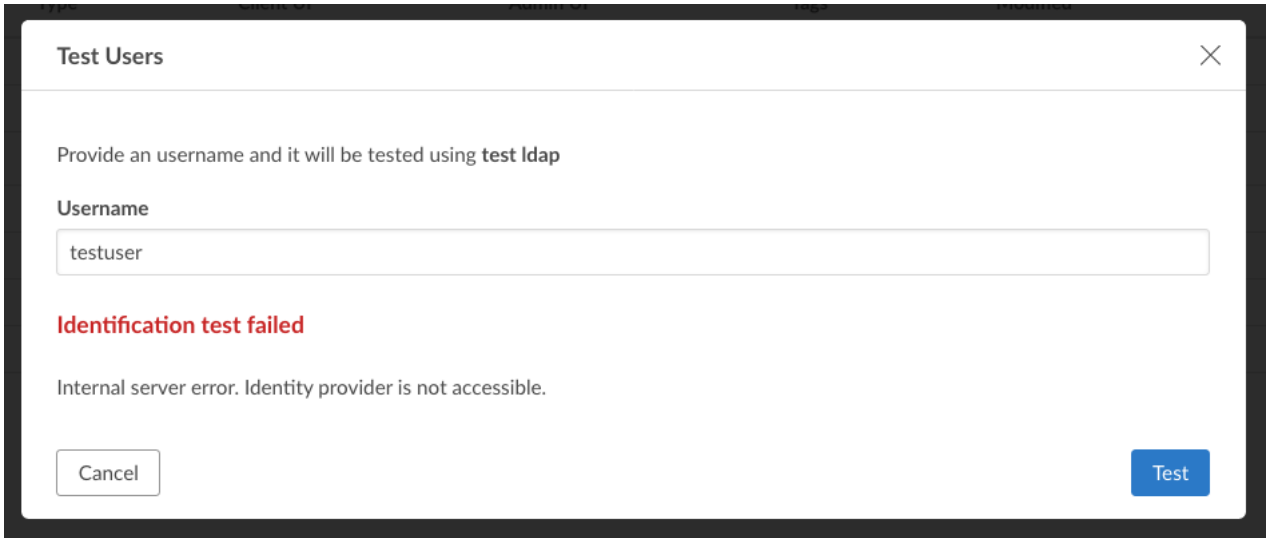


Things to check for:

- Check whether there is an error in the search domain parameters or service account credentials
- Check if there is connectivity between the AppGate SDP Controller and LDAP server, and that port 636 is open
  eg: launch the terminal and use a ping test, and command nc -zv <LDAP IP > 636
- Check if the password of the *Service Account* on your AD server (ie. the admin user credentials for the Controller to log into the AD database) has changed or expired, or the user has been moved to a different group/ou (organizational unit)

Testing user authentication

- When you use the <Test User> icon on the System>Identity Providers console, the following error message indicates that there is a problem, for example:



- Check whether there is an error in the search domain parameters or service account credentials

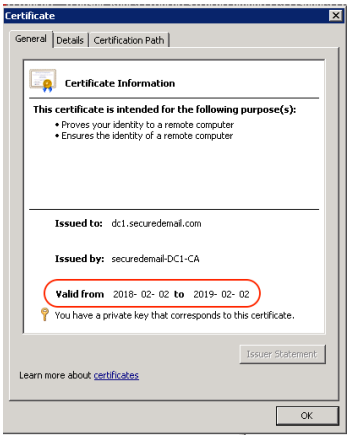
MAINTENANCE

Some changes to your IdP provider or your AppGate SDP configuration may require updating and retesting system integration:

CA certificate expiry:

SSL certificates expire after a predefined lifespan. Knowing when a certificate expires lets you replace or renew the certificate before the expiration date and update the new certificate to your AppGate SDP configuration.

From your AD server administrator panel you can see when the CA certificate will expire:



1. **Renew or create a new certificate:**
- Follow the instructions from your provider to upload a new certificate to your AD server, and export the certificate file to a local drive
2. **Update your AppGate SDP configuration:**
- On your AppGate SDP Controller console, open the **System>Identity Provider** configuration form for your identity provider
  In the *Certificate* field, click the <**Choose a File**> button and upload the Certificate that you exported.
  Save the changes.
3. Test the system integration: repeat the “Testing Integration” steps above.

HELP AND SUPPORT

For more information about the next steps in setting up your AppGate SDP system , refer to the Admin Guide

Please visit the Help Center to browse the knowledge base or log a support ticket for all AppGate products. Learn more about the Help Center below.

Self-service help

Self-service help can be browsed or searched for technical solutions. Browse FAQs, known issues, best practices, service examples, guides and manuals.

Customer support requests

Customers can submit support requests in accordance with their Support and Maintenance contracts. We recommend that you sign in to the support portal and submit from your own support account. If you do not have access, please fill in the “request a login” form available on the Help Centre.

FEEDBACK

If there is any information in this Integration Guide that needs to be updated, or instructions that need further clarification, please let us know. Send your feedback to the Help Center.